REMARKS

I. INTRODUCTION

In response to the Office Action dated January 23, 2008, please consider the following remarks.

II. STATUS OF CLAIMS

Claims 1-2, 4-17, 19-50, and 52-53 are pending in the application.

Claims 1, 5, 14-18, 20, 25-28, 32, 34, 36, 40-43, and 52-53 were rejected under 35 U.S.C. §103(a) as being unpatentable over Okabe et al., U.S. Patent No. 6,889,208 (Okabe) in view of Downs et al., U.S. Patent No. 6,574,609 (Downs).

Claims 2, 4, 29, and 31 were rejected under 35 U.S.C. §103(a) as being unpatentable over Okabe in view of Downs and further in view of Dolphin, U.S. Patent No. 5,677,953 (Dolphin).

Claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 were rejected under 35 U.S.C. §103(a) as being unpatentable over Okabe in view of Downs and in further view of Akins, III et al., U.S. Patent No. 6,560,340 (Akins).

III. GROUNDS OF REJECTION TO BE REVIEWED

Whether claims 1, 5, 14-18, 20, 25-28, 32, 34, 36, 40-43, and 52-53 are patentable under 35 U.S.C. § 103(a) over U.S. Patent No. 6,889,208, issued to Okabe et al. (hereinafter, the Okabe reference) in view of U.S. Patent No. 6,574,609, issued to Downs et al. (hereinafter, the Downs reference).

Whether claims 2, 4, 29, and 31 are patentable under 35 U.S.C. § 103(a) over Okabe in view of Downs and further in view of U.S. Patent No. 5,677,953, issued to Dolphin (hereinafter, the Dolphin reference).

Whether claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 are patentable over Okabe in view of Downs and in further view of U.S. Patent No. 6,560,340 issued to Akins, III et al. (hereinafter, the Akins reference).

IV. ARGUMENT

A. The References

1. The Okabe Reference

U.S. Patent No. 6,839,208, issued May 3, 2005 to Okabe et al. disclose contents sale system. In the contents sale system, original contents data are encrypted into encryption-resultant contents data in response to original playback key data. The original playback key data are encrypted into first encryption-resultant playback key data. The first encryption-resultant playback key data are encrypted into second encryption-resultant playback key data in response to an ID of a sale destination terminal apparatus. The encryption-resultant contents data and the second encryption-resultant playback key data are transmitted to the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the second encryption-resultant playback key data into the first encryption-resultant playback key data in response to the ID of the sale destination terminal apparatus. The sale destination terminal apparatus is enabled to decrypt the first encryption-resultant playback key data into the original playback key data. The sale destination terminal apparatus is enabled to decrypt the encryption-resultant contents data into the original contents data in response to the original playback key data.

2. The Downs Reference

U.S. Patent No. 6,574,609, issued June 3, 2003 to Downs et al. discloses a method of managing content data and associated metadata. According to the method, the content data and the associated metadata are generated. The content data is transferred to a content host, and the metadata and usage condition data for the associated content are transferred to an electronic store. The metadata and/or the usage condition data are altered in order to form promotional data, and the promotional data is transferred from the electronic store to a customer's system. In one preferred method, the content data is encrypted with a first encrypting key before being transferred to the content host. The first encrypting key is encrypted with a second encrypting key, and the encrypted first encrypting key is transferred along with the metadata and usage condition data to the electronic store. Additionally, the encrypted first encrypting key is transferred along with the promotional data to the customer's system.

3. The Dolphin Reference

U.S. Patent No. 5,677,953, issued October 14, 1997 to Dolphin discloses a system and method for access control for portable data storage media that is said to provide the support of high density removable media, such as CD-ROM or MO, to be used as a distributed media for storing data where access thereto is securely restricted. The secure periodic distribution of several different sets of data information to the end user is said to be achieved with access control selectively performed by at the user's site through communication with the billing/access center. User billing is based on the purchase of the decryption access codes as indicated by the access code attributes encoded on the media. Access code availability is further controlled by selectively providing for updates of decryption access codes.

4. The Akins Reference

U.S. Patent No. 6,560,340, issued May 6, 2003 to Akins et al. disclose a method and apparatus for geographically limiting service in a conditional access system. A cable television system includes a headend from which service "instances", or programs, are broadcast and a plurality of set top units for receiving the instances and selectively decrypting the instances for display to system subscribers. The service instances are encrypted using public and/or private keys provided by service providers or central authorization agents. Keys used by the set tops for selective decryption may also be public or private in nature, and such keys may be reassigned at different times to provide a cable television system in which piracy concerns are minimized.

B. Claims 1, 5, 14-18, 20, 25-28, 32, 34, 36, 40-43, and 52-53 are Patentable Under 35 U.S.C. § 103(a) over Okabe in view of Downs

1. Even When Combined, the Okabe and Downs References Do Not Teach the Applicant's Invention

The Applicant has stated that the claimed invention differs from the related prior art in that it encrypts the second (CP) key in the conditional access module instead of the receiver, and does so using a key (CAM key) that is generated or stored internal to the CAM.

The Final Office Action answered:

"The Examiner disagrees with the argument for multiple reasons. First the applicant's arguments are not specifically stated in the claims, the claim does not indicate that a second key is stored in the CAM."

To which the Applicant responds:

With Regard to Whether the Claims Recite that the Second Encryption Key is Encrypted in the CAM: claim 1 unequivocally states that the second encryption key is encrypted in the CAM, specifically "*encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key*"

With Regard to Whether the Claims Recite that the Second Key is Stored in the CAM: The Final Office Action has mistead the Applicant's claims. The key that is used to encrypt the second (CP) key is the third encryption key (the CAM key), not the second encryption key. This feature not explicitly cited in claim 1 or 17, but is expressly recited in claims 26 and 39.

The Final Office Action also states:

"Second the applicant is considering the references individual not in combination."

To which, the Applicant responds:

As the Applicant has stated, *even when combined, the Okabe and Downs do not teach all of the features of the Applicant's claims. Specifically, the functional allocation between the receiver and the CAM described further below.*

Finally, the Final Office Action States:

"Okabe teaches that a key can be stored in a receiver. Downs teaches the distribution of Secure Containers (SC) technology. In Downs the receiver of a SC whether a vendor, distributor, or user computer has the ability to re-encrypt the media to a second, third, and fourth encryption keys."

To which, the Applicant responds:

This statement does not appear to relate to the Applicants invention as claimed, and is therefore unhelpful in understanding why the Applicants claims stand rejected.

We turn now to discuss the individual claim rejections:

a) Claim 1 is Patentable Under 35 U.S.C. § 103(a) Over the Okabe and Downs References

Claim 1 recites:

A method of storing program material in a media storage device communicatively coupled to a receiver for subsequent replay, comprising the steps of:

(a) accepting encrypted access control information and the program material encrypted according to a first encryption key in the receiver, the access control information including a first encryption key and control data;

(b) decrypting the received access control information in a conditional access module releasably coupleable with the receiver to produce the first encryption key;

(c) decrypting the program material in the receiver using the first encryption key;

(d) re-encrypting the program material according to a second encryption key;

(e) encrypting the second encryption key in the conditional access module according to a third encryption key to produce a fourth encryption key; and

(f) providing the re-encrypted program material and the fourth encryption key for storage external to the conditional access module.

Claim 1 allocates functions between the receiver in the CAM. Namely, it specifies that:

The conditional access module:

- decrypts the received access control information to produce a key that is used to decrypt the program material
- encrypts a second key (that was used to re-encrypt the decrypted program material) using third key to produce a fourth key

The conditional access module does not:

- store the re-encrypted program material and the fourth encryption key; and

The receiver:

- is coupled to a media storage device (cited in the preamble) in which the encrypted access control information and the encrypted program material is stored

Returning to the cited references, we note that Downs discloses no functional allocation between hardware elements at all ... all functions are performed by the user's computer. That certainly does not disclose the functional allocation described in claim 1.

Okabe is of no help. As described below, it discloses a system in which the terminal (which the Office Action analogizes to the Applicant's receiver) receives encrypted playback key and encrypted program material, further encrypts the program key, and transmits the encrypted program material and the further encrypted program key to the player (which the Office Action analogizes to the Applicant's CAM).

> A customer's player *6a* can be connected to the terminal apparatus **5** via an IEEE1394 interface. The player *6a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player *6a* to implement processes mentioned later. The player *6a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player *6a*. In the case where the player *6a* is connected with the terminal apparatus **5**, the player *6a* informs the terminal apparatus **5** of its own ID before downloading. The terminal apparatus **5** separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus **5** encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus **5** is connected with the player *6a*, the terminal apparatus **5** downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player *6a*. The player *6a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player *6a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

These functions are not analogous those recited in claim 1 (where nothing is "further encrypted", but rather, decrypted and re-encrypted). The player (CAM) decrypts the encrypted content, but does not store that re-encrypted program material or another key for storage external to the player (CAM) as recited in the last step of claim 1. Instead, it stores it internally.[1]

Accordingly, even when combined, the Downs an Okabe references do not disclose or teach all of the features of claim 1.

The Final Office Action answers:

> "The Examiner disagrees with argument for multiple reasons. Again the applicant is placing limitation that are not present in the claims, the negative limitation argued "that the conditional access module does not store the re-encrypted program material and the fourth encryption key" is not in the claims. Plus the argument does not make sense, obviously if the CAM produces the re-encrypted program material and the fourth encryption key then provides them for storage at some point it has the re-encrypted program material and the fourth encryption key are stored in the CAM registers."

To which the Applicant responds:

---

[1] Storage in a second player does not cure this defect, since what is stored in the second player is not the re-encrypted program material and the fourth encryption key that was recited in the preceding step.

The Final Office Action is correct in that there is no *negative limitation* indicating that "the conditional access module does not store the re-encrypted program material and the fourth encryption key." The Applicant has avoided using such a *negative limitation* because they are somewhat disfavored by the PTO,[2] and because, as the Final Office Action points out, some temporary storage of at least a portion of the re-encrypted program material and the fourth encryption key must be stored at some point. The Applicant was simply attempting to describe, in simple terms, the scope of the invention in terms of the functional allocation between the CAM and the receiver.

Claim 1 plainly recites that the re-encrypted program material are *"provided ... for storage external to the conditional access module."* That feature distinguishes the Applicant's invention from Downs and Okabe, even in combination.

Downs discloses a system where all operations are performed on the user's computer. There is no notion of the use of a receiver or a conditional access module that is releaseably coupleable to it.

Okabe discloses a system with a terminal (analogized to the Applicant's receiver) that receives an encrypted playback key and encrypted program material, further encrypts the program key, and transmits the encrypted program material and the further encrypted program key to a player (which the Office Action analogizes to the Applicant's CAM).

That player (analogized to the Applicant's CAM) decrypts the encrypted content but does not *provide the re-encrypted program material and the fourth encryption key for storage external to the player.* Okabe describes storage in a second player, but what is stored in that second player is not the re-*encrypted program material and the fourth encryption key*, as claim 1 recites in the preceding step. Accordingly, even when combined, Okabe and Downs do not fairly teach or suggest the Applicant's invention.

The Final Office Action also answered: Second Okabe and Downs are analogous art both are directed to digital rights management (DRM).

The Applicant Responds: A rejection based on 35 U.S.C. § 103(a) requires more. In formulating a rejection under 35 U.S.C. § 103(a) based on a combination of prior art elements, it

---

[2] See MPEP 707.07(g) stating that "Certain technical rejections (e.g. negative limitations, indefiniteness) should not be made where the examiner, recognizing the limitations of the English language, is not aware of an improved mode of definition.

remains necessary to identify the reason why a person of ordinary skill in the art would have combined the prior art elements in the manner claimed.

The Final Office Action also answered: Third although applicant is claiming the encryption is done in the conditional access module (CAM) not in a computer like Downs, obviously to do encryption the CAM must contain a CPU just like a computer contains a CPU.

The Applicant Responds: Again, the point is the functional allocation between the receiver and the CAM. Downs and Okabe, even when combined, do not disclose the claimed features.

The Final Office Action also answered: Fourth the applicant is placing limitation not in the claims as well as not considering the entire references of Okabe and Downs both disclose hardware elements, see Okabe col. 6, lines 34-60 which teaches that the content sale system includes a terminal apparatus 5 located in a store (for example, a kiosk or a convenience store). The terminal apparatus includes a computer, communication devices, and an interface for connection with a customer's player. Also see Downs col. 6, lines 59- for an example of the hardware that can receive SC. The applicant's description as well as claimed limitation of the conditional access module (CAM) do not limit the CAM from being a kiosk in a store that the provides a user's player or receiver with encrypted access control information.

The Applicant Responds: Again, the point is the functional allocation between the receiver and the CAM. Even if Okabe's terminal and player could be analogized to the Applicant's "receiver" and "conditional access module" (and in the Applicant's view, they cannot, as a conditional access module is not analogous to a player), Okabe's player does not *provide the re-encrypted program material and the fourth encryption key for storage external to the player.*

As for Downs, the Final Office Action refers to the following passage

> I. SECURE DIGITAL CONTENT ELECTRONIC DISTRIBUTION SYSTEM
> A. System Overview
> The Secure Digital Content Electronic Distribution System is a technical platform that encompasses the technology, specifications, tools, and software needed for the secure delivery and rights management of Digital Content and digital content-related content to an end-user, client device. The End-User Device(s) include PCS, set top boxes (IRDs), and Internet appliances. These devices may copy the content to external media or portable, consumer devices as permitted by the content proprietors. The term Digital Content or

This passage indicates that the Downs system could be implemented in a set top box (IRD) instead of a computer. It also indicates that the content may be copied to portable consumer devices. However, unless such portable playback devices could be said to (1) decrypt the received

access control information to produce a key that is used to decrypt the program material received in the IRD, (2) encrypts a second key (that was used to re-encrypt the decrypted program material using a third key to produce a fourth key, and (3) provides the re-encrypted program material and the fourth encryption key for storage external to the conditional access module, such devices are not analogous to the conditional access module of the Applicant's invention.

In response to applicant's argument beginning on page 19, "It would also not be obvious to modify the Okabe and Downs combination to arrive at the Application's invention ... As a threshold matter, the prior art teaches a different functional allocation than that which is claimed by the Applicant."

2. The Final Office Action Has Not Made a Prima Facie Case for Unpatentability

The Final Office Action proffers the following motivation for modifying Okabe as described in Downs:

> "It would have been obvious to one of ordinary skill in the art at the time of the invention to modify the method of protecting digital content used in distribution taught in '208 to include a controlling the number of copies generated. One of ordinary skill in the art would have been motivated to perform such a modification because content distributors have been slow to embrace digital content distributions systems because of the lack of security for digital content see '609 (col. 2, lines 2-44) "The use of global distribution systems such as the Internet for distribution of digital assets such as music, film, computer programs, pictures, games and other content continues to grow. At the same time owners and publishers of valuable digital content have been slow to embrace the use of the Internet for distribution of digital assets for several reasons. One reason is that owners are afraid of unauthorized copying or pirating of digital content. The electronic delivery of digital content removes several barriers to pirating . . . This degradation in quality is not present when a picture is stored digitally. Each copy, and every generation of copies can be as clear and crisp as the original. The aggregate effect of perfect digital copies combined with the very low cost to distribute content electronically and to distribute content widely over the Internet makes it relatively easy pirate and distribute unauthorized copies. With a couple of keystrokes, a pirate can send hundred or even of thousands of perfect copies of digital content over the Internet. Therefore a need exists to ensure the protection and security of digital assets distributed electronically. Providers of digital content desire to establish a secure, global distribution system for digital content that protects the rights of content owners. The problems with establishing a digital content distribution system includes developing systems for digital content electronic distribution, rights management, and asset protection."

The problems with the foregoing rationale are many. First, the need to protect digital information from copying is conceded to be well known. Both Okabe and Downs protect digital information, yet in different ways.

The issue, of course, is how that data is protected. is that it Okabe itself controls the number of copies generated (e.g. by use of "generation number" that is decremented when the contents is transmitted as shown in FIG. 10 and the accompanying text).

The Final Office Action appears to believe that all that is required to make out a prima facie case of obviousness under KSR is to assure that the references are from the same field of endeavor:

> The Examiner disagrees with argument the applicant's claimed disclosure as well as the prior art references both are directed to digital rights management by encrypting access control information. The KSR ruling indicates it is permissible to combine prior art references from the same endeavor.

This, of course, is not the case. The Final Office Action must provide some defensible reason or rationale for modifying Okabe, and as described above, has failed to do so.

Further, the Applicant has pointed out that the closer prior art (much more analogous to the Applicant's invention than either Okabe or Downs) teaches away from the Applicant's invention

3. The Prior Art Teaches Away from the Applicant's Invention

Consider the Applicant's invention with the system described in EP 0 989 557 A1 (hereinafter, "EP" system), for example. Unlike either of the references relied upon in rejecting the Applicants' claims, this reference discloses a receiver used in conjunction with a removable CAM, and teaches that the second encryption key is encrypted in the receiver, not the CAM.

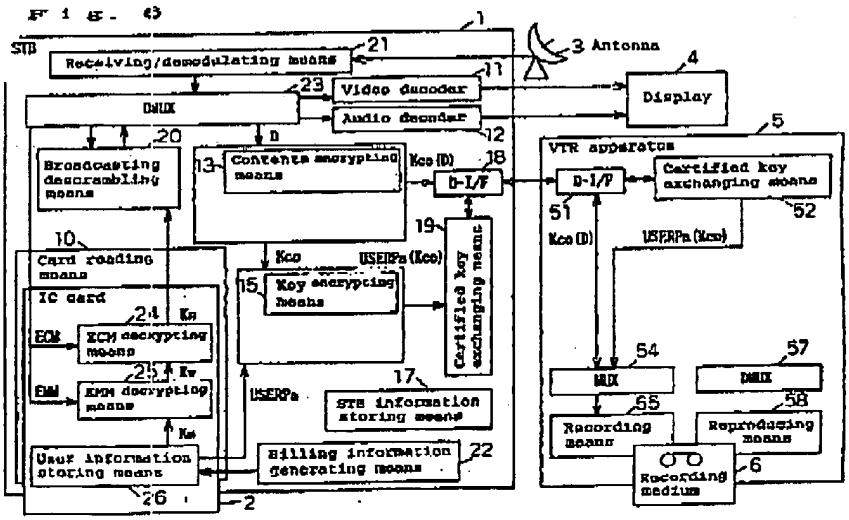
Both systems same the same ultimate goal ... to minimize the possibility of compromising the security of the stored media program ... but only the Applicant's invention achieves it.

The EP system describes the storage of the USERPa key on a smart card that is coupled to an STB before use. Smart cards are well known in the art to include a plurality of electrical connectors that mate with matching connectors in a card reader when the card is inserted into the reader. The EP system discloses such a reader (the card reading means 10). The Applicant's invention also discloses the use of a conditional access module that is coupled to the receiver before use:

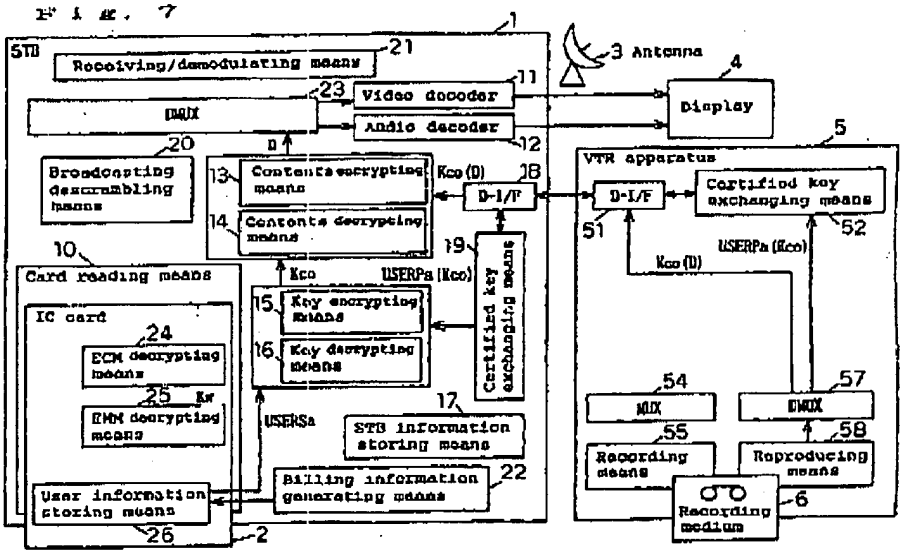
The IRD 132 is communicatively coupleable to a conditional access module (CAM) 406. The CAM 406 is typically implemented in a smart card or similar device, which is provided to the subscriber 110 to be inserted into the IRD 132.

Because the CAM is communicatively coupled to the receiver by the subscriber by inserting it into the receiver, the Applicant's invention is subject to the same problem as the EP system ... the signals passing to and from the CAM may be monitored. In embodiments where the CAM is a smart card (like the EP system), this involves simply monitoring the electrical connectors of the smart card.

Referring to FIG. 6a, below, the EP system transmits a USERPa (user public) key from the smart card to the STB in unencrypted form. The EP system then encrypts the program material with a Kco key, encrypts that Kco key with the USERPa key obtained from the smart card (thus generating USERPa(Kco)), and stores both in the recording medium.



Note that the Kco key cannot be easily monitored by monitoring the link between the contents encrypting means and the key encrypting means (since that is internal to the STB and not passed from the STB to the IC card. However, the unencrypted USERPa key can be monitored directly from on the smart card, leaving it open to compromise. The user's secret key is needed to decrypt the media program as described in FIG. 7 below:



Note that the user's secret key USERSa can also be monitored directly from the smart card, leaving it open to compromise as well.

Also note that the ultimate security of the EP system depends on the user's secret key. If that key is compromised, it can always be used to determine Kco (even if it is time-invariant), and any program material stored in the recording medium 6 can be recovered. In other words, to defeat the entire system, the pirate need only determine the value of USERSa, and that value is not difficult to obtain.

The Applicant's invention encrypts the CP (presumably analogous to Kco) within the CAM instead of the receiver, as shown below:

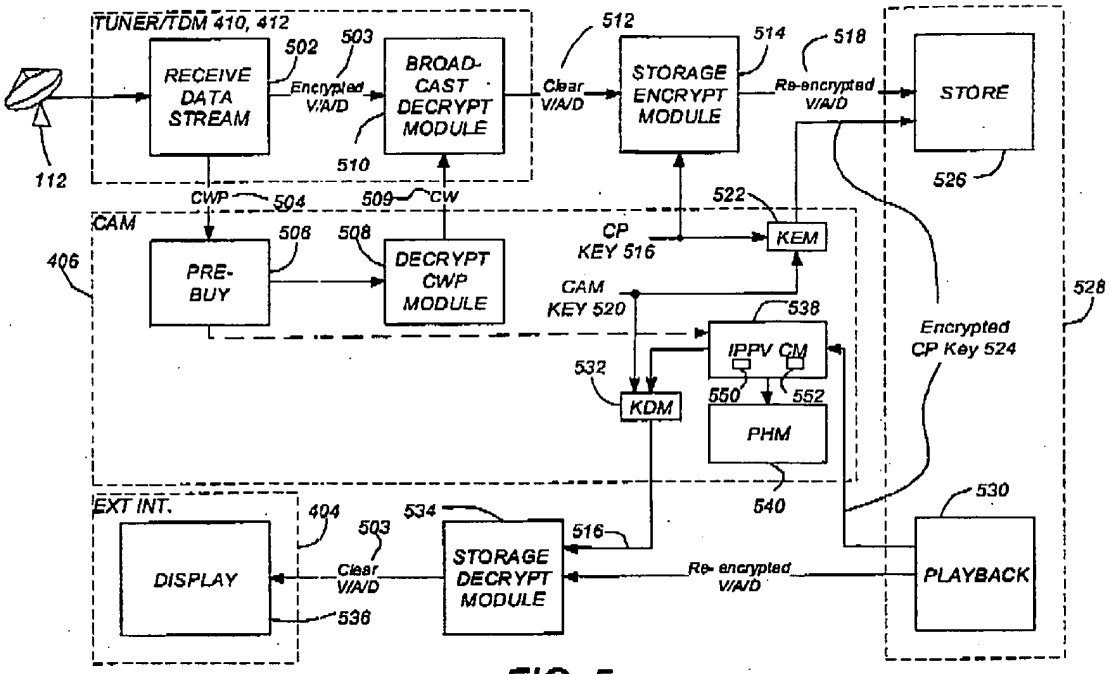


FIG. 5

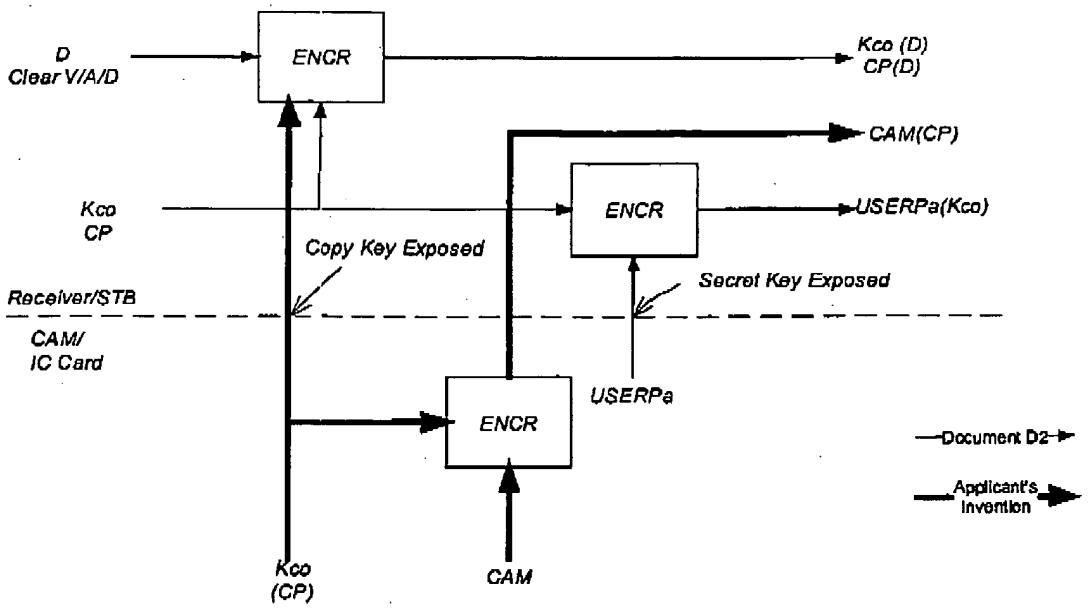
By doing so, the CP key is exposed, because it is passed unencrypted from the CAM to the receiver.[3] However, the CAM key (perhaps analogous to the USERPa or USERSa key) is never exposed. It is always encrypted before leaving the CAM.

This difference is significant. The EP system is less secure because it exposes the heart of it's security (USERSa) by passing it unencrypted from the IC card to the receiver. Once the hacker has gained access to the value of USERSa, they can decrypt *any* program that was stored on the storage medium. Further, since USERSa does not change over time, the hacker need not concern themselves with regenerating a new USERSa over time. It need only be accomplished once.

Contrast this with the Applicant's invention. Because the Applicant's invention exposes the copy protection key CP (perhaps analogous to Kco), but not the CAM key, the Applicant's invention is somewhat vulnerable to a hacker trying obtain the value of CP key, but invulnerable to a hacker attempting to divine the value of the CAM key. This is shown diagrammatically below:

---

3 It may be possible to encrypt this information from the CAM and decrypt it in the receiver, but this additional capability would increase the cost of both the STB and the CAM.



The Applicant's solution is especially well suited to systems wherein the value of the CP key changes over time or changes with the media program. That's because a compromise of the CP key will only allow the hacker to view one program or only a portion of one program. Unlike the EP system, what is compromised does not permit the hacker to view *all* programs.

The Final Office Action responds:

> In response to applicant's explanation of the system described in EP 0 989 557 on pages 19-23, this is irrelevant because as previously noted Okabe and Downs teach the claimed limitations. The EP was not utilized in the rejection; therefore all arguments that address the improvements by the applicant's claimed invention are irrelevant. The 'CAM' comprising a smartcard was not introduced until dependent claim 4. This limitation is taught with the combination of Dolphin US Patent 5,677,953.

To Which the Applicant answers:

EP0989557 is not irrelevant to the patentability of the Applicant's invention. It describes system far more analogous to the Applicant's invention than Okabe or Downs, and is therefore as relevant or more so. It also shows that the prior art, taken as a whole, teaches away from the Applicant's invention.

4. Claim 17 is Patentable over the Okabe and Downs References

Claim 17 recites similar features to those of claim 1. Namely, claim 17 recites a conditional access module that is releasably communicatively coupleable to a tuner, and has (1) a first decryption module for decrypting the received access control information to produce the first encryption key, (2) a first encryption module for encrypting the second encryption key with a third encryption key to produce a fourth encryption key, and (3) a second encryption module for decrypting the fourth encryption key to produce the second encryption key. Claim 1 also recites a tuner for providing re-encrypted program material and the fourth encryption key for storage external to the conditional access module.

Accordingly, claim 17 is patentable for the same reasons as claim 1.

5. Claim 28 is Patentable over the Okabe and Downs References

Claim 28 recites features similar to those of claim 1 and 17 and is patentable for the same reasons.

6. Claims 25 and 26 are Patentable over the Okabe and Downs References

With Respect to Claim 25: Claim 25 recites that the second key is stored in the conditional access module. According to the Office Action, this feature is disclosed as follows:

> A customer's player *6a* can be connected to the terminal apparatus 5 via an IEEE1394 interface. The player *6a* includes a computer which operates in accordance with a control program stored in a memory. The control program is designed to enable the player *6a* to implement processes mentioned later. The player *6a* also includes a storage unit. A predetermined ID (a predetermined identification code word) is assigned to the player *6a*. In the case where the player *6a* is connected with the terminal apparatus 5, the player *6a* informs the terminal apparatus 5 of its own ID before downloading. The terminal apparatus 5 separates the composite data into the primary encryption-resultant playback key data and the encryption-resultant contents data. The terminal apparatus 5 encrypts the primary encryption-resultant playback key data into secondary encryption-resultant playback key data (second encryption-resultant playback key data). In the case where the terminal apparatus 5 is connected with the player *6a*, the terminal apparatus 5 downloads the encryption-resultant contents data and the secondary encryption-resultant playback key data into the storage unit of the player *6a*. The player *6a* recovers original contents data by decrypting the encryption-resultant contents data. In addition, the player *6a* generates other secondary encryption-resultant playback key data (third encryption-resultant playback key data) which will be used for data transfer or data copying to another player.

The second key is the key used to re-encrypt the decrypted program material. The third key is the key used to encrypt the second key (which was used to re-encrypt the program material). Player 6a, which the Office Action appears to analogize to the CAM, does not store a second key used to re-encrypt decrypted program material or a third key used to encrypt the second key. Accordingly, the Applicants traverse the rejection of claim 25 and 26.

The Final Office Action does not appear to further address this rejection.

7. Claims 5, 14-16, 18, 20, 27, 32, 34, 36, 40-43, 52, and 53 are Patentable Over the Okabe and Downs References

Claims 5, 14-16, 18, 20, 27, 32, 34, 36, 40-43, 52, and 53 each recite the features of the independent claims they depend upon, and are patentable for the same reasons.

C. Claims 2, 4, 29, and 31 are Patentable Under 35 U.S.C. § 103(a) over Okabe in view of Downs and further in view Dolphin

Claims 2, 4, 29 and 31 recite the features of the independent claims they depend upon, and are patentable for the same reasons.

D. Claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 are Patentable Under 35 U.S.C. § 103(a) over Okabe in view of Downs and in further view of Akins

The Final Office Action rejected claims 6-13, 19, 21-24, 33, 35, 37-39, and 44-50 under 35 U.S.C. §103(a) as being unpatentable over Okabe in view of Downs in further view of Akins, III et al., U.S. Patent No. 6,560,340 (Akins). Applicants respectfully traverse these rejections.

With Respect to Claims 6, 44-50: Claim 6 recites that the second encryption key is generated at least in part from the metadata. According to the Office Action, this feature is disclosed in the Akins reference as follows.

instance 105. Control word 117 is produced by control word generator 119 from information contained in entitlement control message 107 and information from authorization information 121 stored in set-top box 113. For example, authorization information 121 may include a key for the service and an indication of what programs in the service the subscriber is entitled to watch. If the authorization information 121 indicates that the subscriber is entitled to watch the program of encrypted instance 105, control word generator 119 uses the key together with information from ECM 107 to generate control word 117. Of course, a new control word is generated for each new ECM 107.

Respectfully, this only discloses the use of a control word to determine whether the subscriber is entitled to view a program. It does not even remotely disclose generating the second encryption key (that is used to re-encrypt a program) at least in part from metadata. Further, the motivation to modify Okabe and Downs as described in Akins (more flexibility) doesn't explain how any suggested change would increase flexibility.

There is a significant advantage in generating the second key at least in part from the metadata. It prevents having to generate a random number for the second key, and also assures that the metadata can be later recovered. That recovered metadata can be simply used to control replay or can be compared to the metadata before encryption to assure that the second key has not been tampered with. None of these advantages is even remotely suggested by any of the cited references. Claim 44 recites similar features and is patentable for the same reasons.

Claim 45 recites that the second encryption key is augmented with a least a portion of the metadata before encrypting the second encryption key in the CAM. According to the Office Action, this is disclosed as described above. The Applicants respectfully disagree for the reasons described above, and because the above passage further does not disclose augmenting a key with metadata before encryption. Claim 46 is patentable for analogous reasons.

Claims 47-50 recite analogous features to those above, and are patentable for the same reasons.

The Final Office Action argues:

> The Examiner disagrees with the argument for multiple reasons. One using the broadest reasonable interpretation the 'metadata' was interpreted to be the Entitlement Control Messages which is used by the decryptor to produce a key. Second Akins is directed to DRM as well therefore according to KSR ruling it is permissible to combine the references. Finally the advantages stated in the arguments are not placed in the claims, therefore these arguments are irrelevant.

The Applicant answers that even if were appropriate to interpret "metadata" so broadly as to include an entitlement control message (ECM), Akins does not disclose generating the anything analogous to the Applicant's second encryption key (which is used to re-encrypt a program) at least in part from metadata. Instead, Akins discloses generating a control word that is used to *decrypt* the program using the ECM.

Finally, the Final Office Action has interpreted KSR fat to broadly. KSR does not stand for the proposition that references can be combined for no other reason that they involve analogous arts.

With Respect to Claim 13: Claim 13 recites:

> The method of claim 12, wherein steps (b)-(f) are performed in response to a pre-buy message, and wherein:
>
> the second encryption key and the third encryption key are stored in a smartcard, and the replay right data is generated from the metadata and the pre-buy message in the smartcard; and
>
> the steps of accepting the buy data, comparing the buy data with the replay right data, and decrypting the fourth encryption key using the third encryption key to produce the second encryption key according to the comparison between the buy data and the replay right data are performed in the smartcard.

None of the cited references discloses the functional allocation presented in claim 13.

V. CONCLUSION

In view of the above, it is submitted that this application is now in good order for allowance and such allowance is respectfully solicited. Should the Examiner believe minor matters still remain that can be resolved in a telephone interview, the Examiner is urged to call Applicants' undersigned attorney.

Respectfully submitted,

Date: March 24, 2008

By: _____
Name: Victor G. Cooper
Reg. No.: 39,641

The DIRECTV Group, Inc.
RE/R11/A109
2250 E. Imperial Highway
P. O. Box 956
El Segundo CA 90245

Telephone No. (310) 964-4615